REMARKS

The examiner provisionally rejected Claims 8-13 and 17-22 on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 5-10 of co-pending Application No. 10/701,356.

In the prior Office Action, the examiner furnished the following claim chart:

10/701,154	**10/701,356**
claims 8 and 17	**claim 5**
claims 9 and 18	**claim 6**
claims 10 and 19	**claim 7**
claims 11 and 20	**claim 8**
claims 12 and 21	**claim 9**
claims 13 and 22	**claim 10**

Instant claim 8 and base claim 1 are reproduced below:

> 1. (Previously Presented) A system, comprising:
> a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and
> an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node.
> 8. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address.

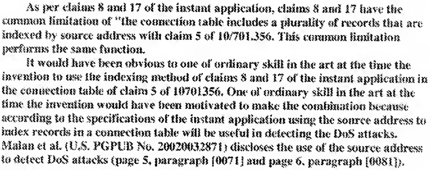
Claim 5 and base claim 1 from 10/701,356 ('356) are reproduced below:

> 1. (Currently Amended) A device, comprising:
> a processor;
> a memory storing a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node.
> 5. (Currently Amended) The device of claim 1 wherein each host object in the connection table maps to a plurality of records that are indexed by source address, the plurality of records

> including host-pair records that map network traffic between pairs of hosts.

In response to the previous action, Applicant had indicated a willingness to consider submission of a terminal disclaimer. However, in view of the current rejection and the state of the claims in '356 application, Applicant responds as follows:

Instant claim 8 requires *inter alia* a plurality of collectors … an aggregator which produces a connection table that includes records indexed by source address. Claim 5 of '356 in contrast calls for a processor and a memory storing a connection table that includes records indexed by source address. The examiner argues that:



As per claims 8 and 17 of the instant application, claims 8 and 17 have the common limitation of "the connection table includes a plurality of records that are indexed by source address with claim 5 of 10/701.356. This common limitation performs the same function.

It would have been obvious to one of ordinary skill in the art at the time the invention to use the indexing method of claims 8 and 17 of the instant application in the connection table of claim 5 of 10701356. One of ordinary skill in the art at the time the invention would have been motivated to make the combination because according to the specifications of the instant application using the source address to index records in a connection table will be useful in detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871) discloses the use of the source address to detect DoS attacks (page 5, paragraph [0071] and page 6, paragraph [0081]).

Applicant contends that merely because claims 8 and 5 share a common feature of: "a connection table" does not make this a proper obvious type double patenting rejection. Indeed, claim 8 of the instant case requires data collectors, which elements are not recited claims 1 or 5 of the '356 application.

The examiner improperly uses the instant specification to teach indexing by source address and also relies on Malan for that teaching. As will be discussed below, Malan does not teach indexing by source address. As for the use of the instant specification, Applicant believes that only the claims of the instant case can be properly used by the examiner. The teachings of the instant specification are not available to the examiner in an obvious type double patenting rejection.

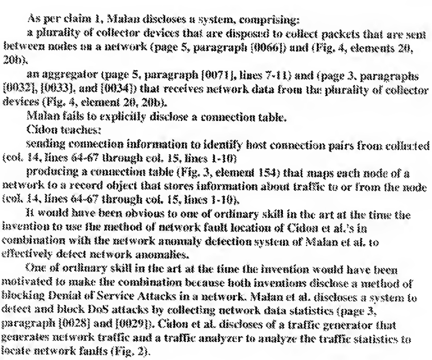
Moreover, it is the data collectors and not indexing that is recited in claim 8, but which is missing in claim 5 of '356. Applicant contends that there is no extension of the monopoly to exclude that would be granted by a patent for the instant case over a patent granted for the '356 application, since the claims of instant case requires data collectors.

A similar analysis holds for claims 9 and 18 of the instant application with claim 6 of '356; claims 10 and 19 of the instant application with claim 7 of '356; claims 11 and 20 of the instant application with claim 8 of '356; claims 12 and 21 of the instant application with claim 9 of '356; and claims 13 and 22 of the instant application with claim 10 of '356.

Therefore, Applicant contends that the rejection is improper and should be withdrawn.

Claim Rejections - 35 U.S.C. § 103

The examiner rejected Claims 1-5, 12-16, and 21-22 under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330).



As per claim 1, Malan discloses a system, comprising:

a plurality of collector devices that are disposed to collect packets that are sent between nodes on a network (page 5, paragraph [0066]) and (Fig. 4, elements 20, 20b).

an aggregator (page 5, paragraph [0071], lines 7-11) and (page 3, paragraphs [0032], [0033], and [0034]) that receives network data from the plurality of collector devices (Fig. 4, element 20, 20b).

Malan fails to explicitly disclose a connection table.

Cidon teaches:

sending connection information to identify host connection pairs from collected (col. 14, lines 64-67 through col. 15, lines 1-10)

producing a connection table (Fig. 3, element 154) that maps each node of a network to a record object that stores information about traffic to or from the node (col. 14, lines 64-67 through col. 15, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time the invention to use the method of network fault location of Cidon et al.'s in combination with the network anomaly detection system of Malan et al. to effectively detect network anomalies.

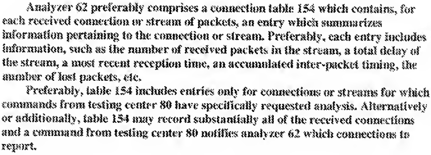
One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking Denial of Service Attacks in a network. Malan et al. discloses a system to detect and block DoS attacks by collecting network data statistics (page 3, paragraph [0028] and [0029]). Cidon et al. discloses of a traffic generator that generates network traffic and a traffic analyzer to analyze the traffic statistics to locate network faults (Fig. 2).

Claim 1

Claim 1 is distinct over Malan et al. (Malan) taken separately or in combination with Cidon since the combination of references neither describe nor suggest *inter alia* ... a plurality of collector devices … to collect connection information to identify host connection pairs from packets that are sent between nodes on a network and an aggregator device … which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node.

The examiner admits that: "Malan fails to explicitly disclose a connection table." The examiner relies on Cidon, col. 14, lines 64-67 through col. 15, lines 1-10 and Fig. 3, element 154.

Applicant contends that Cidon's Fig. 3 merely depicts a box 154, labeled as "connection table." As for Cidon, col. 14, lines 64-67 through col. 15, lines 1-10, those are reproduced below:



> **Analyzer 62 preferably comprises a connection table 154 which contains, for each received connection or stream of packets, an entry which summarizes information pertaining to the connection or stream. Preferably, each entry includes information, such as the number of received packets in the stream, a total delay of the stream, a most recent reception time, an accumulated inter-packet timing, the number of lost packets, etc.**
>
> **Preferably, table 154 includes entries only for connections or streams for which commands from testing center 80 have specifically requested analysis. Alternatively or additionally, table 154 may record substantially all of the received connections and a command from testing center 80 notifies analyzer 62 which connections to report.**

Thus, while Cidon discloses something called "a connection table," Cidon's disclosed "connection table" does not meet the limitations of claim 1. That is, claim 1 requires "an aggregator device that receives the connection information from the … collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node." The connection table described by Cidon does not have these features.

Cidon's table 154 does not describe: "a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node." Rather, Cidon teaches that entries are: "preferably identified by the reference number of the stream or connection."[1] Cidon teaches that: "Alternatively or additionally, commands from testing center 80 may identify or limit the tracking of desired entries using one or more of the arrival time or

[1] Cidon, Col. 15, lines 10-12.

transmittal time of the packets, the identity of the transmitting host, the route or a part thereof through which the packets are passed, the contents of the packets, or any other suitable variables."[2] This explanation of Cidon's connection table clearly shows that there is not any mapping of traffic to or from each node in a network.

The examiner also argues that Malan teaches: "a plurality of collector devices that are disposed to collect statistical information on packets that are sent between nodes on a network (page 5, paragraph [0066]) and (Fig. 4, elements 20, 20b)." Claim 1 however also calls for: "collector devices … to collect connection information to identify host connection pairs … ." This arrangement is not taught by Malan at [0066]. Rather, at [0066] Malan teaches to process data packet flow statistical information to detect data packet flow anomalies.

Applicant contends that one of ordinary skill in the art would not be motivated to make the purported combination because while Malan discloses blocking Denial of Service Attacks, Cidon in contrast is directed to "testing and fault discovery in communication networks,"[3] not to blocking of attacks and in particular DOS attacks. According to Cidon: "Preferably, the traffic agents further include one or more traffic analyzers, which receive data packets or signals from the network and measure and determine the nature, timing and contents of the data according to commands from the testing center."[4]

Thus, the thrust of Cidon's teachings are to fault detection in networks and not to blocking of attacks. Therefore, the examiner's motivation to combine these references must fail because they are directed to different problems and the examiner has not shown why even the different, non-relevant connection table, as mentioned in Cidon would be relevant to the system disclosed by Malan.

Accordingly, no combination of Malan with Cidon describes or suggests Applicant's claim 1.

[2] Id., lines 18-21
[3] Id. col. 1, lines 5-7
[4] Id. Col. 4, lines 8-12

Claim 2

Claim 2 is distinguished over the combination of Malan and Cidon, at least for the reason that it depends from claim 1. In addition, claim 2 requires that … the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions. This feature is not taught by the combination.

The examiner contends that: "Cidon teaches at least in part from the connection patterns derived from the connection table (col. 14, lines 64-67 through col. 15, lines 1-10) and (Fig. 5, evaluate performance of network)." The examiner now acknowledges that Malan does not teach the connection table. Cidon while teaching an item that he refers to as a "connection table," does not teach to determine network events that indicate potential network intrusions based at least in part from connection patterns derived from the connection table. The combination of Malan with Cidon would lead one of ordinary skill in the art to derive occurrences of network events from the statistical data collected by the collectors, since neither Malan nor Cidon teaches one of ordinary skill how to derive occurrences of network events based at least in part on connection patterns. Accordingly, claim 2 serves to further distinguish over Malan and Cidon.

Claim 3

Applicant has amended claim 3 to claim that: "… the aggregator further comprises a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator."

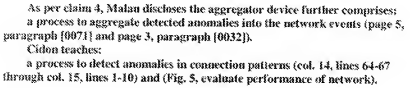
The examiner contends that: "As per claim 3, Malan discloses the aggregator further comprises: a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator (page 6, paragraph [0075], lines 8-13 and page 7, paragraph [0086], lines 1-10)."

Claim 3 recites an analogous feature as that disclosed by Malan, namely, collection of statistical information on packet flows. Claim 3, however distinguishes over Malan and Cidon, since no combination of Malan with Cidon describes or suggests that that aggregator receives both "the statistical information and the connection information," as required by claim 3.

Claim 4

Claim 4 recites that: "the aggregator device further comprises: a process to detect anomalies in connection patterns; and a process to aggregate detected anomalies into the network events."

The examiner contends that:



> **As per claim 4, Malan discloses the aggregator device further comprises:**
>
> **a process to aggregate detected anomalies into the network events (page 5, paragraph [0071] and page 3, paragraph [0032]).**
>
> **Cidon teaches:**
>
> **a process to detect anomalies in connection patterns (col. 14, lines 64-67 through col. 15, lines 1-10) and (Fig. 5, evaluate performance of network).**

While Malan mentions anomalies at paragraph [0071] and again at [0110], no combination of Malan with Cidon suggests: "…to aggregate detected anomalies into the network events."

Claims 12 and 13

Claim 12, which recites that … the connection table includes a plurality of connection sub-tables to track data at different time scales and claim 13, which recites that … wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time … with each sub-table holding the sum of records received … during respective units of time, are each distinguishable over Malan taken with Cidon, since no combination of these references suggests the connection table, per se or a connection table arranged in sub-tables according to time scales.

The examiner argues that: "As per claims 12 and 21, Cidon discloses the connection table (Fig. 3, element 154) includes a plurality of connection sub-tables (col. 5, lines 23-24, nodal tables) to track data at different time scales (col. 14, lines 64-67 through col. 15, lines 1-10)."

However, the passage at col. 5, lines 23-24 mentions nothing concerning "sub-tables to track data at different time scales" and the passage at col. 14, lines 64-67 through col. 15, lines 1-10, while mentioning what Cidon terms a connection table again is silent on the aspect of claim 12 namely, "sub-tables to track data at different time scales."

Claim 13, which recites … sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time …, is allowable at least because of the reasons given in claim 12, namely that Cidon does not teach sub-tables according to time scales and therefore would not inherently teach sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table … .

Claim 5 is allowable at least for the reasons given in claim 1, claims 14-16 are allowable for analogous reasons given in claims 1, 3 and 4. Claims 21-22 are allowable for analogous reasons given in claim 12 and 13.

The examiner rejected Claims 6 and 7 under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330) and further view of Hill et al. (U.S. Patent No. 6,088,804).

Claims 6 and 7 are allowable over the combination of references at least for the reasons discussed in claims 4 and 1 and because Hill does not cure the deficiencies of Malan and Cidon.

The examiner rejected Claims 8-11 and 17-20 under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PUB No. 20020032871) in view of Cidon et al. (U.S. Patent No. 6,269,330) and further view of Chi et al. (U.S. Patent No. 5,940,870).

> **The examiner stated:**
>
> **As per claims 8 and 17, Cidon discloses the connection table (Fig. 3, element 154) Malan in view of Cidon fails to explicitly disclose indexing by address.**
>
> **Chi teaches:**
>
> **includes a plurality of records that are indexed by source address (col. 5, lines 29-43).**
>
> **It would have been obvious to one of ordinary skill in the art at the time the invention to use the network anomaly detection system of Malan et al. in combination with the translating address method of Chi et al.'s to effectively address mapping tables of a multi-computer cluster.**
>
> **One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking security attacks in a network. Malan et al. discloses a database for recording source and destination of packet flows in the network (page 5, paragraph [0067]). Chi et al. discloses a mapping table that stores the source and destination information of the network nodes (Fig. 8). Network statistical information is used to efficiently identify the source and destination nodes of the network (Chi, col. 3, lines 33-37) and (Malan, page 5, paragraph [0067], lines 10-14).**

Applicant contends that claims 8-11 and 17-20 are allowable over the combination of references.

Using claim 8 as an example, claim 8 requires that: "…the connection table includes a plurality of records that are indexed by source address." The examiner acknowledges that Malan taken with Cidon do not suggest this feature and relies on Chi to teach this feature, specifically citing to Col. 5, lines 29-43. In that passage, Chi discusses an address translation map table and specifically an AMT index and offset as an address formation into the table. While, Chi mentions the word "index" Chi does not describe any indexing of a connection table according to source address. Rather, Chi describes address translation involving shared and global memories in a multiprocessor or clustered computer system. No combination of Malan with Cidon and Chi however suggest the desirability of the claimed connection table indexed according to source addresses.

Applicant contends that is an improper application of hindsight using Applicant's claims as a roadmap to find pick and choose teachings various references. In addition, the motivation proffered by the examiner, namely, "…Chi et al. discloses a mapping table that stores the source and destination information of the network nodes (Fig. 8). Network statistical information is used to efficiently identify the source and destination nodes of the network (Chi, col. 3, lines 33-37) and (Malan, page 5, paragraph [0067], lines 10-14)." is inadequate.

It is not suggested to combine Chi with Malan and Cidon, since Chi does not teach that "Network statistical information is used to efficiently identify the source and destination nodes of the network," as the examiner contends, whether at col. 3, lines 33-37 or elsewhere. Rather, at that passage, Chi teaches that at a source node an address on a bus consists of an AMT index and an offset. Moreover, this motivation is not directed to the claimed invention, which is to provide a connection table indexed by source address to retrieve a record that stores information about traffic to or from the node.

In addition, Malan also does not teach that "Network statistical information is used to efficiently identify the source and destination nodes of the network" at page 5, paragraph [0067], lines 10-14, as the examiner contends.

Accordingly the motivation is inadequate and even if adequate, the combination of references do not suggest the claimed features.

Similar arguments apply to claims 9-11 and 17-20.

The examiner rejected Claims 23 and 24 under 35 U.S.C. 102(e) as being anticipated by Belissent (U.S. Patent No. 6,789,203).

The examiner stated:

> **As per claim 23, Belissent discloses a method of detecting a new host connecting to a network comprises:**
>
> **receiving statistics collected from a host in the network (Fig. 6) and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17). Belissent discloses a system for monitoring connection request rates over a period of time and a rejection threshold.**

Belissent neither describes nor suggests … receiving statistics collected from a host in the network and indicating … that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.

Belissent teaches at (col. 4, lines 9-20) throttling the processing of new connections to thwart a denial of service attack, not the detection of new host connecting to a network. Thus for these reasons and the reasons of record, as pertaining to Belissent the claim is allowable.

The examiner stated:

> **As per claim 24, Belissent discloses a method of detecting a failed host in a network comprises:**
>
> **determining if both a mean historical rate of server response packets from a host is greater than M, and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and indicating the host as a potential failed host if both conditions are present (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17).**

Belissent whether at col. 4, lines 9-20; col. 5, lines 62-67 through col. 6, lines 1-17 or elsewhere, neither describes nor suggests … determining … if both a mean historical rate of server response packets from a host is greater than M and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R … and indicating the host as a potential failed host if both conditions are present.

At col. 4, lines 9-20 Belissent discusses IP throttling designed to prevent denial of service attacks, whereas at col. 5, lines 62-67 through col. 6, lines 1-17 Belissent discusses connection request rate throttling. Nowhere does Belissent teach the features of claim 24, e.g., to detect a failed host, and in particular determining the two conditions of claim 24 to indicate a potential failed host if both conditions are present.

The prior art cited but not applied is seen as neither describing nor suggesting Applicant's invention whether taken alone or in combination with the applied art.

No fee is believed due. If a fee is due, please apply that fee and any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 4/26/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906